AFFIDAVIT OF PROBABLE CAUSE

I, Kendra Leanne Holloway, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

1. Your Affiant is a Special Agent (SA) with the Federal Bureau of Investigations (FBI) assigned to the office of the Resident Agent in Charge, Bismarck, North Dakota. Your Affiant has been employed by the FBI since August 2016. Your Affiant has participated in numerous federal and state search warrants and has drafted hundreds of reports of investigation. Your Affiant has successfully completed the Special Agent Basic Field Training Course in Quantico, VA.

2. As a Special Agent, your Affiant is responsible for enforcing federal criminal statutes including the sexual exploitation of children, pursuant to Title 18, United States Code (USC). Your Affiant has received training and actual experience relating to Federal Criminal Procedures, Federal Statutes, and FBI Regulations. Your Affiant has received training and instruction in the field of investigation and has had the opportunity to participate in investigations relating to the sexual exploitation of children. The information contained within the affidavit is based on your Affiant's training and experience, and information obtained from other law enforcement agents involved with this investigation including FBI Special Agent Dan Alfin, assigned to the Miami Field Office. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not set forth all of your Affiant's knowledge about this matter.

3. This Affidavit is made in support of an application for a warrant to search

the Apple iPhone S, Model MKRY2LL/A, Serial Number F4LQGJ9VGRY9, bearing a black and copper in color case.

4. The IPhone S is more particularly described in Attachment A of this Affidavit.

5. Based on your Affiant's training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the Specified Federal Offenses further identified as 18 U.S.C. §§ 2251, 2252(a)(2), 2252(a)(4)(B), 2252(b)(1) and 2252(b)(2), which make it a crime to produce, receive, distribute, or possess child pornography, or attempts to do so, have been committed by the subject of this investigation. There is also probable cause to search the IPhone S described in Attachments A for evidence of these crimes.

6. Because this Affidavit is being submitted for the limited purpose of establishing probable cause, your Affiant has not included every detail of every aspect of the investigation. Rather, your Affiant has set forth only those facts that she believes are necessary to establish probable cause to search the iPhone S listed in Attachment A. Unless specifically indicated, all conversations and statements described in this Affidavit are related in substance and in part.

7. As a result of the investigation described more fully below, there is probable cause to believe that evidence, contraband, and fruits of, and other items related to, violations of the Specified Federal Offenses, are present within the IPhone S as described in Attachment A.

DEFINITIONS

8. Based on your Affiant's training and experience, your Affiant uses the following technical terms to convey the following meanings:

a. **Computer**: The term "computer" means "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." See 18 U.S.C. §§ 2256(6) and 1030(e)(1). As used herein, a computer includes a cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet. The term "computer," including any cell phone, smart phone, tablet, and other similar devices capable of accessing the Internet, is used throughout this affidavit interchangeably with the term "electronic storage device."

b. **Computer Hardware**: The term "computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices such as video gaming systems, electronic music playing devices, and

mobile phones); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

c. **Computer Passwords and Data Security Devices**: The term "computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

d. **Computer Software**: The term "computer software" means digital information which can be interpreted by a computer and any of its related

components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

e. **Computer-Related Documentation**: The term "computer-related documentation" means written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

f. **Exif data**: The term "exif data" refers to 'Exchangeable Image File" data and it is the information that a camera stores in relation to the picture taken. This information may include date and time information, camera settings such as the camera model and make, information about the image that varies with each image, a thumbnail for previewing the picture on the camera's LCD screen, in file managers, or in photo manipulation software, etc.

g. **Internet**: The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. **Internet Connection**: The term "Internet connection" means a connection required for access to the Internet. The connection would generally be

provided by cable, DSL (Digital Subscriber Line), wireless devices, or satellite systems.

i. **Internet Service Providers**: The terms "Internet Service Providers" or "ISPs" mean commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

j. **Minor**: The term "minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

k. **Storage Medium**: The term "storage medium" refers to any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

l. **Visual Depictions**: "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

m. **Wireless Network**: The term "wireless network" means a system of wireless communications in which signals are sent and received via electromagnetic waves such as radio waves. Each person wanting to connect to a wireless network needs a computer which has a wireless network card that operates on the same frequency. Many wired networks base the security of the network on physical access control, trusting all the users on the local network. But, if wireless access points are connected to the network, anyone in proximity to the network can connect to it. A wireless access point is equipment that connects to the modem and broadcasts a signal. It is possible for an unknown user who has a computer with a wireless access card to access an unencrypted wireless network. Once connected to that network, the user can access any resources available on that network to include other computers or shared Internet connections.

BACKGROUND ON COMPUTERS, CHILD EXPLOITATION AND THE INTERNET

9. Your Affiant has both training and experience in the investigation of computer-related crimes. Based on your Affiant's training, experience, and knowledge, and conversations with other law enforcement personnel familiar with these types of investigations, your Affiant knows the following:

a. Computers and digital technology have dramatically changed the way in which individuals interested in exploiting children interact with each other. Computers basically serve four functions in connection with child exploitation: communication between persons engaging in child exploitation to arrange and accomplish the exploitation and also for the production, distribution, and storage of child pornography which is often directly associated with child exploitation. Often times a person who is engaged in seeking out a child to exploit on the internet will store images of the exploited child in electronic format.

b. The computer's ability to store images in digital form makes the computer itself an ideal repository for images of child exploitation. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is

extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person or in an individual's vehicle.

c. The Internet affords individuals several different venues for persons involved in the exploitation of children to meet and communicate and also for obtaining, viewing, and trading child pornography, all in a relatively secure and anonymous fashion.

d. Individuals can use online resources (such as Yahoo! and Hotmail, among others) to communicate regarding child exploitation and also retrieve and store child pornography or other images. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of the exploitation of minors using the internet and/or child pornography can be found on the user's computer or external media in most cases.

e. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

f. Individuals often carry on their person, or in their vehicles, smartphones and other electronic storage devices. These devices are sometimes the same devices which they use to exploit children on the internet or may contain evidence related to the sexual exploitation of children.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

10. Based upon your Affiant's training and experience and information related to your Affiant by agents and others involved in the forensic examination of computers, your Affiant knows that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. Your Affiant also knows that during the search of a premises, it is not

always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

10. Based on your Affiant's own experience and your Affiant's consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit (CPU). In cases like the instant one where the evidence consists partly of

image files, the monitor and printer are also essential to show the nature and quality of the graphic images which the system could produce. Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

11. Your Affiant knows that electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction, a controlled environment is essential to ensure its complete and accurate analysis.

12. Additionally, based upon your Affiant's training and experience and information related to your Affiant by agents and others involved in the forensic examination of computers, your Affiant knows that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are sometimes instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may

yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, your Affiant knows that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

13. Your Affiant knows that graphic image files sent and received during the online exploitation of children and those containing child pornography can be maintained for long periods of time in a number of ways: on a computer's hard disk drive, on portable storage disks, on CDs, or on other computer storage media. Most often an individual who has a sexual interest in children maintains the files purposefully and will use the images for fantasy or sexual gratification. Even when the image files have been deleted, computer forensic experts are nonetheless often able to recover the images that had been purposefully possessed previously.

14. Your Affiant knows that people who use personal computers in their homes tend to retain their personal files and data for extended periods of time; months or even years. Due to a personal computer's unique ability to store large amounts of data for extended periods of time without consuming much additional physical space; people tend to retain this data. Your Affiant knows this to be true regardless of whether or not a person has traded-in or "upgraded" to a new personal computer. Personal computer

users routinely transfer most of their data onto their new computers when making an upgrade. This data transfer is often done by saving files from the old computer to media sources (CDs or floppy disks, etc.) and then saving them to the new hard drive. Visual images, such as those sent and received during communications regarding child exploitation as well as child pornography, are as likely as other data to be transferred to a person's new, replacement or upgraded computer system.

15. Your Affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools.

16. Based on your Affiant's training and experience, your Affiant knows that data or particularly images can be received by use of a home computer and transferred to other electronic devices, such as a cell phone. Your Affiant also knows that data or images can be received by use of a cell phone and transferred to a home computer or other electronic storage devices.

17. Your Affiant is aware that conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies for a standard computer can take several business days. Complex systems or recover tasks can require much longer time periods. Due to the backload of computers waiting to be examined and

the limited number of trained examiners, any item seized pursuant to this warrant may be examined outside the regular time period as dictated by the addendum to this warrant.

SUMMARY OF INVESTIGATION

18. On or about January 2018, an FBI Task Force Officer (TFO) working for Plantation, Florida Police Department obtained a laptop computer from a minor male and consent to search the laptop from the minor child's mother. On February 5, 2018, while reviewing data on the aforementioned laptop, FBI Special Agent Dan Alfin observed Skype conversations between the minor in Florida and Skype username "ethanbagg38." According to Skype logs, on April 17, 2017, "ethanbagg38" sent the minor in Florida several messages via Skype including messages stating "I would suck u dry," "Wanna see my sons cock?," and "Isn't that the cutest thing you ever saw?"

19. According to data from the Florida minor's computer, on that same day, April 17, 2017, "ethanbagg38" sent several images to the minor in Florida including a photo of himself and a series of pictures that appear to depict a minor male sleeping. One picture is focused on the minor's exposed nude genitals. It appears the blanket and his underwear were pulled back so the picture could be taken while he slept. The blanket appears to be a fairly unique looking fuzzy blue blanket. Other messages from "ethanbagg38" state that he planned to engage in future abuse of his son, including drugging his son.

20. On February 5, 2018, SA Alfin conducted a search utilizing the internet website Google.com of the Skype username "ethanbagg38," which revealed a LinkedIn account for Ethan Baggett, Manager at Mattress Firm, from Bismarck, ND, and a

Facebook Profile account for Ethan Baggett, Manager at Mattress Firm in Bismarck, ND. Both the Profile pictures from the aforementioned LinkedIn account and Facebook account appear to match the picture that username "ethanbagg38" sent to the minor of himself.

21. On February 5, 2018, FBI Staff Operations Specialist conducted a search of the Criminal Justice Information Sharing database for the State of North Dakota relative to the name "Ethan Baggett," Bismarck, ND. The aforementioned search revealed Ethan Allan Baggett, Date of Birth XX/XX/1970, with a physical address of 723 N. 11th Street, Bismarck, North Dakota, and a North Dakota Driver's License Number of BAG-70-3935. A review of the driver's license photo associated with the above named individual revealed the person in Ethan Allan Baggett's driver's license photo appeared to be the same individual in the photo that username "ethanbagg38" sent to the minor.

22. On February 5, 2018, your affiant and FBI Task Force Officer (TFO) Steven Takacs conducted surveillance at Mattress Firm, 1495 E LaSalle Drive, Bismarck, North Dakota. During the surveillance, both your affiant and TFO Takacs observed a male individual working inside Mattress Firm who matched the known description and photographs of Ethan Allan Baggett. At approximately 8:15pm, your affiant and TFO Takacs observed Baggett exit Mattress Firm and enter a 2004 Orange Pontiac Grand Am bearing North Dakota Tag 931BXY. Your affiant and TFO Takacs observed as Baggett drove the car to a nearby Wal-Mart, after which he then drove the vehicle to a residence located at 723 N. 11th Street, Bismarck, North Dakota.

23. In February 6, 2018, federal agents executed a search warrant for Baggett's residence, located at 723 N. 11th street, Bismarck, North Dakota. Baggett was not present at the residence at the time of the search. As a result of the search of Baggett's residence, and pursuant to the search warrant, several computers and digital storage devices were seized for further examination by a forensic expert.

24. Baggett was located at his place of employment, The Mattress Firm, located at 1495 E LaSalle Drive, in the city of Bismarck. After being advised of his rights, Baggett agreed to talk to your affiant and SA Randy Helderop, HSI. During the interview Baggett admitted that he indeed took pictures of H.M.'s genitalia, a 14-year-old minor, but did not recall using the internet to transmit the images to Plantation, Florida. Baggett admitted taking similar images of the child on multiple occasions. Baggett stated he believed he utilized his cell phone to take the images, and consented to providing his Apple iPhone S to SA Randy Helderop and your affiant.

25. In light of this information, your Affiant requests the Court's permission to search the aforementioned Apple iPhone S which is believed to contain some or all of the evidence described in the warrant; and to conduct a forensic search of the image or hardware for the evidence of fruits and instrumentalities of violations of the Specified Federal Offenses.

CONCLUSION

26. Based on the above information, there is probable cause to believe that the Specified Federal Offenses have been violated. Accordingly, your Affiant respectfully

requests that this Court issue a search warrant for the aforementioned Apple IPhone S more particularly described in Attachment A, which constitutes evidence, contraband, fruits, and other items related to violations of the Specified Federal Offenses.

FURTHER YOUR AFFIANT SAYETH NOT

Kendra L. Holloway
Special Agent
Federal Bureau of Investigations

Subscribed and sworn to me this 8 day of February, 2018, via telephone.

Alice R. Senechal, U.S. Magistrate Judge
Magistrate Judge, United States District Court